IDENTITY THEFT DENGAN MENGGUNAKAN SOCIAL ENGINEERING

STUDI KASUS: KARTU KREDIT DI INDONESIA

PROPOSAL PENELITIAN

Disusun oleh:

LUCKY ADHIE

Jurusan Teknik Informatika

Fakultas Teknologi Informasi dan Sains

Universitas Katolik Parahyangan

ABSTRAK

Dalam perkembangan perbankan, transaksi kartu kredit semakin marak digunakan baik dalam transaksi nyata maupun didunia maya. Dengan perkembangan ini memunculkan banyak kasus carding, sehingga kartu kredit Indonesia ditolak di beberapa situs yang ternama seperti amazone. Maraknya carding ini disebabkan karena social engineering yang dilakukan beberapa pihak dengan berlaku sebagai pihak bank yang berkedok mengadakan undian atau menyamakan data atau pembuatan kartu kredit baru. Modus-modus sosial engineering apalagi yang digunakan oleh pihak yang tidak bertanggung jawab untuk mencuri identitas. Beberapa data juga dapat dengan mudah diperoleh jika kita menggunakan internet. Melalui situs pertemanan sosial seseorang juga dapat memperoleh banyak data penting yang bisa digunakan untuk memferifikasi ke pihak bank untuk mengubah PIN dan lain-lain. Melalui survey yang akan dilakukan diharapkan dapat melihat bagaimana pandangan dari masyarakat Indonesia terhadap data-data pribadi yang mereka miliki dan bagaimana data dapat dengan mudahnya diperolah oleh pihak yang tidak berkepentingan. Selain itu akan dibahas bagaimana cara melindungi diri dari pencurian identitas.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULAN

1.1. Latar Belakang

Identitas adalah sesuatu yang dimiliki oleh setiap orang. Seseorang dapat dikenali melalui identitasnya. Identitas adalah suatu yang tidak dapat dipisahkan dari seseorang karena identitas dapat membedakan orang yang satu dengan orang yang lainnya, karena dalam identitas melekat beberapa atribut yang dimiliki oleh seseorang seperti misalnya nama, tempat tanggal lahir, alamat dan atribut lainnya.

Pencurian identias adalah sesuatu yang sulit dilakukan pada jaman dahulu karena seseorang harus menyamar dalam arti yang sebenarnya baik dari raut wajah, nada bicara dan seluruh penampilannya harus mencirikan orang sedang diperankan (dalam hal ini yang sedang dicuri identiasnya). Namun sekarang dengan adanya teknologi dan banyaknya transaksi di dunia nyata maka pencurian identitas dapat dilakukan dengan cara yang cukup mudah yaitu dengan mencuri data-data pribadi dari orang tersebut. Dan cara untuk memperoleh data seseorang dapat diperoleh dengan cukup mudah terutama di lingkungan masyarakat yang kurang peka terhadap nilai dari data pribadi seseorang seperti di Indonesia.

Banyak kasus *carding* di Indonesia adalah bukti bahwa masyarakat seringkali tidak sadar akan perlunya seseorang untuk dapat menjaga kerahasiaan beberapa informasi yang dibutuhkan oleh seseorang untuk melakukan transaksi di dunia maya dengan menggunakan kartu kredit. Kasus ini memang bukan kasus baru di dunia karena di Amerika saja sudah banyak korban yang jatuh akibat pencurian identitas ini. Yang menarik adalah data-data tersebut dapat dicuri dengan menggunakan apa yang disebut sebagai *Social Engineering*.

1.2. Pertanyaan Penelitian

Pertanyaan dalam penelitian ini adalah :

- Apa itu *Identity Theft* / Pencurian Identitas?
- Apakah yang dimaksud dengan *Social Engineering*?
- Bagaimana data-data pribadi untuk proses verifikasi kartu kredit dapat diperoleh oleh seorang pencuri identitas?
- Bagaimana masyarakat Indonesia memandang data pribadi mereka?
- Bagaimana melindungi diri dari Pencurian Identitas yang menggunakan *Social Engineering* ?

1.3. Tujuan Penelitian

Tujuan dari penulisan makalah ini adalah memberikan informasi sehubungan dengan pencurian identitas dan *social engineering*. Selain itu akan diperlihatkan modus apa yang dilakukan oleh seorang pencuri identitas untuk memperoleh data-data yang diperlukan untuk dapat melakukan transaksi dengan kartu kredit. Hal lain yang akan diperhatikan adalah bagaimana masyarakat dapat memandang data-data mereka yang bersifat pribadi yang seringkali digunakan oleh pihak Bank sebagai alat verifikasi dalam transaksi kartu kredit serta bagaimana seseorang dapat melindungi diri dari pencurian identitas.

1.4. Batasan Masalah

Batasan masalah dalam makalah ini adalah :

- Pencurian Identitas yang dibahas adalah yang berkaitan dengan penggunakan identitas dalam transaksi di dunia maya
- Survei akan dilakukan kepada 100 responden sebagai data sample yang dapat dikelompokan atas dua jenis responden yaitu :
    - Responden yang memiliki latar belakang pendidikan di bidang sains
    - Responden yang memiliki latar belakang pendidikan di bidang sosial

1.5. Hipotesa

Hipotesa penelitian ini adalah memperlihatkan modus dan faktor-faktor yang akan di manfaatkan oleh para pencuri identitas.

1.6. Teori yang digunakan

Dasar teori yang digunakan pada penelitian ini adalah:

a. Identity Theft/Pencuri Identitas.

b. Nilai dari data pribadi.

c. Social Engineering

1.7. Motodologi Penelitian

Metodologi penelitian secara rinci dijabarkan pada Bab 3, yang intinya adalah:

Berikut ini adalah langkah-langkah yang akan dilakukan dalam penerapan sistem pembayaran mikro:

a. Melakukan studi pustaka mengenai: Identity Theft dan Social engineering.

b. Melakukan observasi dan analisis kasus-kasus penipuan kartu kredit di Indonesia.

c. Melakukan survey dengan menyebarkan quisioner untuk melihat tren dari kerahasiaan informasi bagi masyarakat indonesia

d. Memberikan rekomendasi cara menghindari penipuan

1.8. Keluaran Penelitian

Hasil penelitian ini berupa:

a. Hasil observasi dan analisis tentang kasus-kasus penipuan kartu kredit di indonesia

b. Laporan quisioner yang memperlihatkan tren kerahasiaan informasi.

c. Rekomendasi cara menghindari penipuan

BAB II
Landasan Teori

2.1. Identity Theft

2.1.1 Definisi Identity Theft

Menurut USSA Educational Fondation *Identity Theft* dapat didefinisikan sebagai :

> *Pencurian identitas yang terjadi saat seseorang menggunakan nama, alamat, nomor Jaminan Sosial (SSN), bank atau kartu kredit nomor rekening atau informasi pribadi lainnya, tanpa izin, untuk melakukan penipuan atau kejahatan lainnya* [1].

Encarta Dictionary mendefinisikannya sebagai :

> *"theft of personal information such as somebody's credit card details"*

Merriam-Webster mendefinisikan *identity theft* sebagai :

> *"the illegal use of someone else's personal information (as a Social Security number) in order to obtain money or credit"* [2]

Dari beberapa definisi yang diperlihatkan diatas maka kita dapat menyimpulkan bahwa Identity Theft atau pencurian identitas adalah upaya dari seseorang yang menggunakan data diri seseorang tanpa ijin atau mengambil keuntungan atau penipuan dari menyamar sebagai orang lain dengan menggunakan data-data pribadi tersebut.

Indentity Theft sering kali menyerang para pengguna kartu kredit karena pada transaksi kartu kredit data pribadi selalu digunakan untuk menverifikasi transaksi pembayaran. Oleh karena itu transaksi pembayaran dengan menggunakan kartu kredit adalah salah satu modus yang sangat diminati oleh para pencuri identitas.

Korban dari pencurian identitas tiba-tiba menemukan bahwa seseorang sedang menggunakan banyak uangnya, menipu kreditor, dan menyebabkan kekacauan lain dengan menggunakan nama korban. Di beberapa negeri (seperti Amerika), hukum melindungi korban agar tidak membayar tuntutan-tuntutan ini, tetapi mereka dapat berakhir dengan reputasi yang rusak dan tidak lagi dipercaya untuk diberi kredit. Lembaga-lembaga penegak hukum, orang-orang yang memiliki akses ke informasi konfidensial dalam industri perkreditan, dan kelompok-kelompok konsumen secara luas mengakui bahwa pencurian identitas menyebabkan kerugian miliaran dolar per tahun. Tidak ada cara untuk mengetahui dengan tepat berapa banyak orang yang dicurangi lewat pencurian identitas. Salah satu problem terbesarnya adalah bahwa bisa saja seseorang tidak tahu bahwa identitasnya sudah dicuri sampai berbulan-bulan kemudian. Beberapa lembaga penegak hukum menyebut pencurian identitas sebagai kejahatan yang paling cepat merajalela di Amerika Serikat. Problem yang sama dilaporkan juga di negara-negara yang lain [3]

Pencuri identitas biasanya mencuri satu atau lebih potongan-potongan kunci dari data pribadi Korban, seperti nomor KTP atau surat izin mengemudi. Kemudian, mereka menggunakannya untuk menjadi diri si Korban dan membuka rekening kredit menggunakan nama Korban. Pada saat yang sama, mereka menyimpangkan kertas-kertas catatan yang menyusul akibat transaksi itu ke kotak pos mereka (biasanya alamat penagihan kartu kredit dialihkan ke alamat pencuri sehingga korban tidak menyadari). Mereka menghabiskan sebanyak dan secepat mungkin uang itu. Korban tidak akan tahu apa yang sedang terjadi sampai tagihan datang.

Para pelaku pencurian identitas bisa jadi sangat sulit untuk dikenali karena mereka tidak harus cocok dengan profil tertentu. Tidak ada yang bisa mencirikan seseorang adalah seorang pencuri identitas karena seorang pelaku bisa menjadi orang asing, seorang kasir yang berpikiran kriminal atau penyedia layanan, tetangga atau bahkan anggota keluarga. Oleh karena itu kita memiliki tindakan yang preventif terhadap pihak-pihak yang tidak berkepentingan yang berupaya memperoleh informasi tentang data-data pribadi yang kita miliki.

2.1.2 Nilai Data Pribadi

Seberapa pentingkah data pribadi seseorang, ini merupakan pertanyaan yang sangat sulit dijawab karena apakah kita akan menjadi orang yang tertutup dan selalu penuh kecurigaan ketika seseorang ingin mengenal kita lebih dekat. Data pribadi dapat mendekatkan orang yang satu dengan yang lainnya namun bukan tidak mungkin data pribadi juga dapat digunakan oleh pihak yang tidak berkepentingan dan bahkan yang berniat jahat untuk melakukan suatu tidak kejahatan dengan menggunakan data pribadi yang bisa saja kita anggap tidak penting. Kebanyakan orang meremehkan identitas kita. Kita tahu siapa kita, dan jika ditantang, kita dapat membuktikannya. Namun, alat yang sering kita gunakan sebagai bukti atas identitas kita—akta kelahiran, nomor identitas, surat izin mengemudi, paspor, kartu tanda penduduk, dan semacamnya—semakin mudah untuk dipalsukan atau dicuri.

Dengan teknologi internet seseorang dapat semakin mudah mencari informasi untuk memenuhi kebutuhannya misalnya informasi barang, informasi terkini suatu produk dan lain-lain. Internet juga semakin digunakan oleh masyarakat untuk menjalin hubungan sosial dengan situs jejaring sosial seperti : *Friendster*, *Facebook* dan lain-lain. Untuk dapat menjalin hubungan yang lebih baik seorang pengguna situs jejaring sosial seringkali mencantumkan data pribadi selengkap mungkin dalam profil dirinya. Melalui pencantuman porfil yang lengkap dapat membantu seseorang untuk menemukan orang yang memiliki kesamaan dengannya yang terdapat dalam situs jejaring sosial tersebut, beberapa bahkan mencantumkan informasi yang sangat-sangat lengkap. Namun disisi lain ini akan memudahkan seseorang untuk mencuri identias. Dengan mudahnya seorang yang berniat mencuri identitas dapat menggunakan situs jejaring sosial untuk mendapatkan data-data pribadi yang juga menjadi data yang diisikan pada formulir aplikasi kartu kredit.

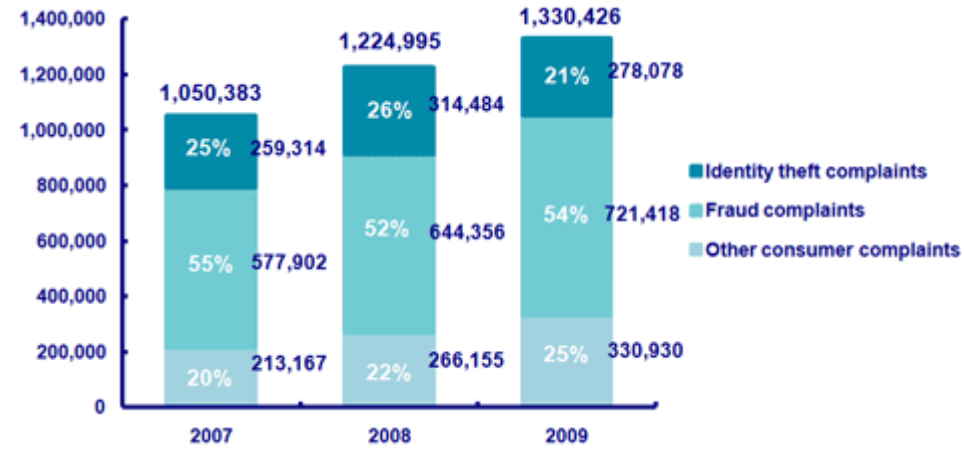
2.1.3 Beberapa Kasus Identity Theft di Amerika

Federal Trade Commission(FTC) baru-baru ini studi menemukan bahwa 8.300.000 orang Amerika adalah korban pencurian identitas di tahun 2005, dan jumlah ini meningkat. Sekurang-kurangnya setengah dari kejadian tersebut, pencuri memperoleh barang atau jasa senilai $ 500 atau kurang, namun untuk 10 persen kasus, pencuri mendapat setidaknya $ 6.000 senilai barang atau jasa. [4]

Lima puluh enam persen dari semua korban tidak dapat memberikan informasi tentang bagaimana informasi pribadi mereka telah dicuri. Identitas pencuri

menggunakan informasi pribadi untuk menyamar sebagai korban, mencuri dari rekening bank, menetapkan kebijakan asuransi palsu, membuka kartu kredit yang tidak sah atau memperoleh pinjaman bank yang tidak sah. [4]

Penggunaan kartu kredit curian dan nomor kartu debit adalah salah satu bentuk yang paling umum dari pencurian identitas. Beberapa skema menggunakan sarana elektronik, termasuk penipuan online seperti *phishing*[1] sementara yang lain akan menggunakan metode yang lebih kuno, seperti *dumpster diving*[2] mereka berada disekitar tempat sampah korban untuk mengumpulkan informasi keuangan.



Source: Federal Trade Commission.

Gambar 2.1. Identity Theft and fraud Complaints USA, 2007-2009 [4]

Pada Gambar 2.1. diperlihatkan bahwa tingkat pencurian identitas pada tahun 2007 sampai dengan tahun 2009 berada dilevel lebih dari 20 persen dari keluhan yang dilaporkan oleh para konsumen. Dan Tabel 2.1. memperlihatkan suatu hal yang lebih memprihatinkan lagi yaitu dari 21% mereka yang melaporkan kasus pencurian identitas atau dari sekitar 278.078 kasus terdapat 17% nya (sebagai kasus tertinggi) dilaporkan menjadi korban pencurian identitas yang melibatkan penggunaan kartu kredit. Ini berarti sebanyak 47.273 kasus merupakan pencurian identitas dengan mengunakan kartu kredit.

[1] menggunakan surat/email yang seolah-olah datang dari perusahaan atau misalnya bank
[2] Mencari berkas-berkas konfidensial dan berguna di tempat sampah

Tabel 2.1. How Victims'Information is Misused, 2009 [4]

Type of identity theft fraud	Percent
Credit card fraud	17
Government documents or benefits fraud	16
Phone or utilities fraud	15
Employment-related fraud	13
Bank fraud (2)	10
Attempted identity theft	6
Loan fraud	4
Other identity theft	23

Source: Federal Trade Commission.

2.2. Social Engineering

2.2.1 Definisi Social Engineering

Menurut European Network and Information Security Agency menyatakan bahwa *Social Engineering* sebagai :

> *"teknik yang digunakan untuk mengeksploitasi kelemahan manusia dan memanipulasi seseorang untuk melanggar prosedur keamanan normal. Ini mungkin melibatkan meyakinkan mereka untuk melakukan tindakan tertentu atau untuk membocorkan informasi rahasia. Serangan tersebut telah menjadi masalah lama dalam domain keamanan, dan pada dasarnya diakui bahwa jauh lebih mudah untuk mengeksploitasi pengguna sistem daripada teknologi itu sendiri."* [5]

Menurut Sarah Granger yang telah merangkumkan beberapa pendapat tentang *social engineering* dapat didefinisikan dengan :

> *"Seni dan ilmu untuk membuat orang lain untuk memenuhi keinginan Anda"* [6]

Dan menurut beberapa sumber yang dikutip dalam makalah dari Rhodes disebutkan bahwa:

"Social engineering melibatkan mendapatkan informasi sensitif atau akses yang tidak sah dari suatu priviledges dengan membangun hubungan kepercayaan dengan orang dalam. Ini adalah seni orang memanipulasi dengan berbicara / bertindak bertentangan dengan cara normal. Itu Tujuan dari seorang social engineering adalah untuk menipu seseorang untuk menyediakan informasi yang berharga atau akses ke informasi tersebut. Mereka memanfaatkan perilaku manusia, seperti keinginan untuk membantu, sikap mempercayai orang dan takut terlibat dalam kesulitan. Tanda bahwa scoial engineering berhasil dilakukan adalah bahwa mereka menerima informasi tanpa kecurigaan." [5]

Sebagai contoh, Institut Keamanan Komputer membuat sebuah survey tahun 2007 tentang Kejahatan Komputer dan Keamanan, hampir setengah dari 475 responden (48%) melaporkan pengeluaran kurang dari 1% dari anggaran keamanan Teknologi Informasi untuk pelatihan *employee awearness,* dan hanya9% yang mengaku berinvestasi lebih dari 5% dari anggaran mereka ke arah ini (CSI, 2007). Fokus utama pada aspek teknis dari keamanan dan keyakinan bahwa kerentanan manusia dapat dengan mudah dikontrol masih tidak mampu mencegah insiden. Para pembobol seringkali mencari titik terlemah dari kemanan sistem dan ternyata karyawan dengan kelemahan manusiawinya merupakan bagian yang seringkali diserang. Kevin Mitnick, salah satu hacker yang paling terkenal pada 1980-an dan 1990-an, lebih berhasil dalam menggunakan kemampuannya untuk memanipulasi orang daripada keterampilan teknis sebagai hacker. Mitnick sendiri mengamati, jauh lebih mudah untuk mengelabui seseorang untuk mengungkapkan password mereka daripada melakukan hack yang rumit untuk tujuan yang sama. [5]

2.2.2 Beberapa Trik yang Digunakan dalam Social Engineering

Social engineering bisa melibatkan baik psikologis dan teknologi untuk meningkatkan kepercayaan target. Dari perspektif psikologis, penyerang dapat memanfaatkan beberapa karakteristik perilaku manusia dalam rangka meningkatkan peluang korban untuk melakukan apa yang diinginkan.Terdapat enam dasar prinsip yang dapat mempengaruhi individu untuk memenuhi permintaan [5]:

1. *Authority* - penyerang mencapai respon yang diinginkan dari target dengan membuat sebuah pernyataan otoritas

2. *Commitment and Consistency* - sasaran akan bertindak secara konsisten dengan perilaku di masa lalu, dan sesuai dengan hal-hal yang telah mereka kerjakan.

3. *Liking and Similarity* - penyerang memanfaatkan fakta bahwa target lebih cenderung untuk menanggapi seseorang yang mereka suka, atau yang dianggap mirip dengan diri mereka sendiri.

4. *Reciprocation* - target diberikan sesuatu, dengan harapan bahwa mereka akan merasa berkewajiban untuk membalas dengan memberikan sesuatu sebagai balasannya.

5. *Scarcity* - target dipandu untuk percaya bahwa sesuatu yang mereka inginkan adalah langka atau hanya tersedia untuk jangka waktu terbatas. Target akibatnya mungkin merasa berkewajiban untuk bertindak cepat dan tanpa berpikir panjang.

6. *Social validation* - target membuat keputusan mereka atas perilaku orang lain (kemungkinan permintaan yang dipenuhi akan meningkat dengan mengklaim bahwa orang lain juga telah melakukan hal yang sama).

Dari enam prinsip dasar inilah korban dieksploitasi dan hal ini dapat mendukung pada keinginan dari seseorang yang bermaksud jahat dengan memanfaatkan kelemahan sosial manusia pada umumnya.

Teknik *Impersonation*/Peniruan ini bisa dibilang teknik yang sering digunakan oleh para social engineering untuk menipu orang, misalnya dengan menyamar sebagai seorang karyawan dari organisasi yang sama. Kebanyakan orang pada dasarnya rela membantu, sehingga tampaknya tidak berbahaya untuk mengatakan kepada seseorang yang lupa dimana ruang komputer terletak, atau membiarkan orang yang lupa tanda pengenal atau lencananya untuk masuk ke gedung atau lantai tertentu. [7]

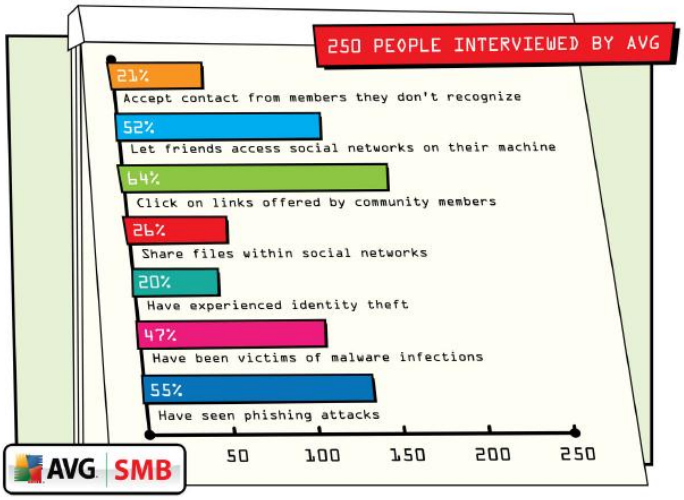
Menggunakan telepon untuk melakukan serangan *social engineering* tidak hanya sering digunakan di tempat kerja, tetapi juga telepon dapat menjadi sarana untuk memperoleh informasi pribadi dari orang-orang di rumah. Suatu hal yang umum bagi seseorang untuk menerima panggilan telepon di rumah dari perusahaan kartu kredit tentang *account* mereka. Oleh karena itu, orang sering tidak takut untuk

mengungkapkan informasi tentang *account* mereka kepada seseorang melalui telepon yang mengaku mewakili perusahaan kartu kredit mereka. Dikebanyakan kasus, tujuan serangan *social engineering* yang ditujukan pada seseorang di rumah adalah untuk memperoleh informasi nomor kartu kredit seseorang, nomor KTP, dan / atau nomor rekening bank. Dalam banyak kasus, para pelaku *social engineering* bisa mendapatkan informasi ini dengan menawarkan sesuatu yang bernilai untuk pemegang kartu misalnya dengan iming-iming hadiah atau dengan menggunakan rasa takut bahwa *account*-nya berada dalam bahaya.

2.2.3 Beberapa Kasus Social Engineering

Kasus *social engin*eering yang sangat terkenal adalah Kevin Mitnick, ia telah mengakui bahwa *social engineering* adalah bagian mendasar dari pendekatannya. "Bila rata-rata orang melukisan bagaimana rupa seorang hacker komputer, yang biasanya muncul dalam benak seseorang adalah seorang yang kesepian, *introvert*, aneh dan teman yang terbaik yang dimilikinya adalah komputernya dan seringkali memiliki kesulitan dalam percakapan sehari-hari, kecuali pesan instan ". Mitnick menjelaskan dalam bukunya The Art of Deception. "Para pelaku *social engineering*, adalah hacker yang keterampilan teknis namun ia juga memiliki keterampilan sosialisasi yang baik dan menggunakannya dalam memanipulasi orang, sehingga cara ini memungkinkan pelaku untuk berbicara seperti biasa untuk mendapatkan informasi dalam cara-cara Anda tidak akan pernah percaya mungkin." [8] Kevin Mitnick dalam aksinya telah merugikan banyak pihak jutaan dolar amerika.

Dalam Gambar 3.1. diperlihatkan hasil Wawancara AVG terhadap beberapa orang yang telah mengalami kejahatan komputer dan 21 persen menerima kontak dari member yang belum mereka kenal dalam jejaring sosial ini memberi gambaran bahwa dengan mudah seorang pelaku so*cial engineering* dapat melakukan aksinya. Dimulai dengan menerima member yang tidak dikenal di jejaring sosial dapat berlajut ke pencarian data yang lebih intensif lagi melalui *social engineering*.



Gambar 3.1. AVG Interview [8]

BAB III
METODA PENELITIAN

3.1. Studi Literatur

Pada fase studi pustaka akan dilakukan studi mengenai Indetity Theft dan Social Engineering sehingga dapat memiliki pemahaman yang lengkap tentang modus yang digunakan.

3.2. Melakukan Observasi dan analisis kasus-kasus penipuan kartu kredit di Indonesia

Pada fase ini akan dilakukan observasi terhadap kasus-kasus penipuan kartu kredit di Indonesia. Selain itu akan dibahas juga modus yang digunakan oleh para pencuri identitas dan penipu kartu kredit.

3.3. Melakukan survey dengan menyebarkan quisioner untuk melihat tren dari kerahasiaan informasi bagi masyarakat indonesia

Pada fase ini akan dilakukan survey dan penyebaran quisioner terhadap masyarakat yang melibatkan berbagai pihak baik akademisi maupun masyarakat umum dan akan dilihat perbedaan nilai informasi bagi masyarakat yang memiliki latar belakang sosial dan sains.

3.4. Memberikan rekomendasi cara menghindari penipuan

Pada fase ini akan diberikan rekomendasi cara menghindari penipuan yang terjadi akibat rentannya kerahasiaan informasi.

BAB IV
IDENTITY THEFT DENGAN MENGGUNAKAN SOCIAL ENGINEERING DALAM KASUS KARTU KREDIT

4.1. Kasus Pencurian Identitas dan Penipuan Kartu Kredit di Indonesia

Di Indonesia pencurian identitas sangat sering ditemukan dalam kasus penyalahgunaan Kartu Kredit. Dalam berbagai kasus di terangkan bahwa proses penyalahgunaan kartu kredit yang sering disebut dengan carding di indonesia. Bank Indonesia mencatat sejumlah pemalsuan dan penipuan *"fraud"* kartu kredit di Indonesia antara Januari dan Oktober 2009 mencapai 7.654 kasus. Tipe *"fraud"* antara lain kartu palsu, kartu hilang atau dicuri, kartu tidak diterima, *"Cardholder-Not-Present/CNP"*, fraud aplikasi (pemalsuan identitas pemilik dalam aplikasi kartu kredit), dan *"Mail Only Telephone Only/MOTO"* [9]. Hal ini terus meningkat dengan semakin meningkat dari hari ke hari karena semakin banyaknya perdagangan data pribadi oleh pihak ketiga. Karena tingginya tingkat penipuan dan pencurian identias dalam kasus kartu kredit maka banyak situs e-commerce yang besar seperti Amazone pemah memberlakukan pelarangan pembelian untuk kartu kredit yang berasal dari bank-bank Indonesia. Melalui anlisis yang dilakukan kasus pecurian indentitas di indonesia dengan menggunakan ,social engineering terasa lebih mudah dilakukan karena :

1. **Budaya:** budaya Indonesia yang menekankan gotong royong dan suka membantu walaupun orang itu baru dikenal, sehingga dapat dengan mudah dimanfaatkan oleh para pencuri identitas.

2. **Pengetahuan :** rendahnya tingkat pengetahuan yang dimiliki oleh masyarakat Indonesia tentang modus-modus yang digunakan untuk penipuan kartu kredit, sehingga para pencuri identitas dapat memperoleh data dengan mudah

3. **Kepercayaan :** Mudah untuk percaya kepada orang-orang yang baru dikenal terutama bila orang tersebut cukup meyakinkan.

4. **Ketakutan :** rata-rata masyarakat indonesia mudah ditakut-takuti oleh sesuatu yang tidak dimengerti sehingga jika ada pelaku yang mencoba menakut-nakuti dapat dengan mudah terpengaruh.

5. **Konfidensialitas data:** masyarakat indonesia tidak merasa bahwa data pribadi mereka adalah sesuatu yang penting, bahkan password yang merupakan sesuatu informasi yang bersifat rahasia seringkali di *share* dengan orang lain.

Sebuah survey dilakukan pada 2 kelompok responden yang memiliki latar belakang yang berbeda yaitu mereka yang berlatar belakang Ilmu Eksakta dengan mereka yang berlatar belakang Ilmu Sosial.

Kuisioner dilakukan dengan mengajukan 13 pertanyaan berikut ini :

Bagian 1

Suatu hari ada telepon dari seorang yang menyatakan dirinya sebagai pegawai dari sebuah Bank. Dia menyatakan tujuannya menelepon adalah untuk melakukan pendataan ulang. Pegawai tersebut mengajukan beberapa pertanyaan (*Silakan pilih jawaban "**YA**" jika anda akan memberitahukan data tersebut, dan jawab "**TIDAK**" jika anda menolak untuk memberitahukan data yang diminta*)

Bisakah anda menyebutkan

1. No Kartu Kredit anda :
    a. YA b. TIDAK
2. Nama yang tertera pada Kartu :
    a. YA b. TIDAK
3. Masa berlaku Kartu :
    a. YA b. TIDAK
4. 3 angka yang terdapat pada belakang Kartu (dekat tanda tangan):
    a. YA b. TIDAK
5. Limit Kartu Kredit anda :
    a. YA b. TIDAK
6. Tempat Tanggal Lahir :
    a. YA b. TIDAK
7. No telpon rumah :
    a. YA b. TIDAK
8. Nama Ibu Kandung :
    a. YA b. TIDAK
9. Alamat rumah anda :
    a. YA b. TIDAK
10. Alamat email anda :
    a. YA b. TIDAK
11. Andaikata pegawai tersebut menyatakan akan mengambil fotocopy KTP anda, apakah anda akan memeberikan fotocopy KTP/SIM anda :
    a. YA b. TIDAK

Bagian 2

Jika anda bertemu dengan stand Bank tertentu atau pribadi tertentu yang menyatakan dari pihak Bank dan menawarkan untuk mengajukan Kartu kredit dengan iuran bulanan gratis lalu ia meminta anda untuk mengisi formulir maka :

12. Jika pegawai tersebut meminta KTP dan Kartu Kredit lain apakah akan diberikan:
    a. YA b. TIDAK
13. Apakah anda akan mengijinkan jika pegawai tersebut memfotocopy bagian belakang dari kartu anda:
    a. YA b. TIDAK

Hasilnya dapat terlihat dari Tabel 4.1. dan Tabel 4.2

Tabel 4.1. Hasil Kuisioner dari Bidang llmu Eksakta

Pertanyaan	Ya	Tidak
1	6%	94%
2	34%	66%
3	20%	80%
4	0%	100%
5	23%	77%
6	54%	46%
7	23%	77%
8	20%	80%
9	11%	89%
10	57%	43%
11	6%	94%
12	23%	77%
13	9%	91%

Tabel 4.2 Hasil Kuisioner dari Bidang Ilmu Sosial

Pertanyaan	Ya	Tidak
1	47%	53%
2	62%	38%
3	58%	42%
4	18%	82%
5	36%	64%
6	64%	36%
7	69%	31%
8	58%	42%
9	62%	38%
10	60%	40%
11	33%	67%
12	22%	78%
13	11%	89%

Tabel 4.2 Hasil Kuisioner Gabungan

Pertanyaan	Ya	Tidak
1	29%	71%
2	50%	50%
3	41%	59%
4	10%	90%
5	30%	70%
6	60%	40%
7	49%	51%
8	41%	59%
9	40%	60%
10	59%	41%
11	21%	79%
12	23%	77%
13	10%	90%

Perbandingan dari Tabel 4.1. dan Tabel 4.2. memperihatkan bahwa mereka yang memiliki latar belakang Eksakta lebih sentitif terhadap data dan introvert sehingga mereka lebih berhati-hati terhadap mereka yang menanyakan data-data pribadi mereka hal ini berbeda dengan mereka yang memiliki latar belakang sosial yang cendrung lebih terbuka dan *ekstrofert* terhadap orang lain sehingga data dengan mudahnya diberikan kepada pihak yang sedang melakukan *social engineering*.

Tabel 4.3. memperlihatkan sesuatu yang dapat memberikan kita alasan mengapa tingkat pencurian identitas di Indonesia sangat tinggi terutama dalam kasus carding. Masih ada masyarakat (10 persen) yang memberikan data untuk pertanyaan no 4 yang serupa dengan tanda tangan atau ,yang disebut dengan *Verification and Validation Plan* (VVP).

Dengan memperoleh angka VVP ini transaksi kartu kredit dapat dengan mudah dilakukan (karena nomor kartu kredit lebih mudah diperoleh). Hal lain yang seringkali digunakan untuk melakukan reset pin adalah nama Ibu kandung. Data data lain seperti limit kartu kredit dan waktu berlaku juga merupakan salah satu sarana untuk melakukan verifikasi data ketika akan mengubah PIN atau melakukan transaksi online.

Social engineering juga dapat dilakukan dengan berpura-pura menjadi pegawai bank yang menawarkan jasa pembuatan aplikasi kartu kredit yang baru. Beberapa pelaku bisa saja mengambil form aplikasi yang biasanya digunakan oleh pihak Bank untuk dapat diisi oleh calon nasabahnya. Di Indonesia formulir aplikasi ini dapat tersebar dimana saja.sehingga membuat pelaku social engineer lebih mudah meyakinkan korbannya. Dengan formulir ini

seseorang akan memberikan data selengkap mungkin dan bahkan beberapa memberikan atau mengijinkan kartu kreditnya di fotokopi di Tabel 4.3 pertanyaan ke 12 dan 13 memberikan gambaran jika seseorang berminat mengajukan aplikasi kartu kredit yang baru maka fotokopi kartu kredit yang dimiliki pun dapat diberikan walaupun nilainya hanya rentang 10-23 persen namun bayangkan angka ini jika dikalikan dengan 1.000 orang.

4.2. Modus Pelaku

Para pelaku identity theft dengan mengunakan social engineering untuk kasus penyalahgunaan kartu kredit biasanya berperan sebagai seseorang yang bekerja di sebuah Bank yang menerbitkan kartu tersebut. Mereka bisa saja berperan sebagai bagian pemasaran sebuah produk kartu kredit yang memiliki program menarik sehingga korban tanpa merasa curiga dan memberikan semua data pribadi yang dibutuhkan. Yang paling sering dilakukan adalah melalui telepon. Seorang pelaku *social engineering* bisa saja mengaku sebagai seorang pegawai dari suatu Bank dan menjelaskan bahwa terdapat perubahan sistem sehingga PIN harus segera di reset atau korbannya diminta untuk menyamakan data dengan menggunakan PIN yang mereka miliki. Karena perasaan takut beberapa korban bisa saja tanpa merasa curiga memberikan nomor PIN nya dan hal ini sangat menguntungkan para pelaku.

Te1epon juga digunakan untuk menawarkan ap1ikasi kartu kredit sedang marak di Indonesia sehingga ini bisa dimanfaatkan oleh pelaku *social engineering* untuk melakukan pencurian identitas. Mereka bisa saja bermodus menawarkan aplikasi kartu kredit lalu diminta agara melengkapi data yang mereka minta, untuk hal ini mereka tidak pemah menanyakan no PIN namun bisa saja mereka meminta informasi kartu kredit lain yang aktif yang bisa diguakan untuk proses pengajuan aplikasi. Setelah berhasil mendapatkan databisa saja pelaku menyatakan akan mengambil fotokopi KTP dan tanda tangan dari si korban atau bahkan fotokopi rekening koran yang berisi data-data kartu kredit. lni di dilakukan oleh sang pelaku agar memiliki data yang semakin lengkap. Karena seseorang bisa me-reset PIN dengan mengajukan permohonan perubahan PIN via telepon dengan cara menyamakan data.

4.3. Cara Menghindari Penipuan

Menurut suatu sumber kita perlu melakukan beberapa langkah berikut ini agar tidak menjadi korban dari pencurian identitas [3] yaitu:

- Berikan nomor KTP hanya kalau memang benar-benar perlu.

- Jangan membawa kartu kredit tambahan, KTP, akta kelahiran, atau paspor dalam dompet, kecuali hila diperlukan.
- Sobek-sobeklah formulir permohonan kredit yang akan disetujui sebelum membuangnya. Sobeklah juga rekening bank, telepon, kuitansi kartu kredit, dan semacamnya.
- Gunakan tangan Anda sebagai penutup sewaktu menekan nomor pada A TM atau sewaktu menelepon jarak jauh menggunakan kartu. "Shoulder surfer" bisa saja berada di sekitar situ, mengamati dengan binokular atau kamera.
- Milikilah kotak surat yang dapat dikunci, guna mengurangi pencurian surat.
- Ambillah cek-cek baru di bank, daripada menerimanya melalui pos.
- Simpanlah daftar atau fotokopi dari semua nomor rekening kredit di tempat yang aman.
- Jangan pernah memberikan nomor kartu kredit Anda atau informasi pribadi lainnya lewat telepon kecuali Anda memiliki hubungan bisnis yang dapat dipercaya dengan perusahaan tersebut atau Anda yang menelepon.
- Hafalkan kata sandi Anda. Jangan menyimpan catatan tertulis berisi kata sandi di dompet Anda.
- Dapatkan salinan laporan kredit Anda secara rutin jika mungkin.
- Singkirkan nama Anda dari daftar promosi yang dioperasikan oleh biro pelaporan kredit dan pihak-pihak yang memberikan kredit.

Saran diatas tidak bermaksud untuk membuat seseorang menjadi orang yang anti sosial dan cendrung berprasangka atau introfert tetapi ini adalah saran yang bisa ditempuh karena modus penipuan yang semakin beragam dan meningkatnya kejahatan diranah tersebut.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Kesimpulan yang didapat dari penelitian ini adalah :

- Kasus *indentity theft* dengan menggunakan *social engineering* di Indonesia sangat mudah dilakukan karena karakter masyarakatnya yang cendrung menerima dengan terbuka orang asing.
- Terdapat perbedaan karakter dalam memandang data antara seseorang yang berlatar belakang ilmu eksakta dan ilmu sosial.
- Perlu upaya untuk melindungi diri dari praktek penipuan yang menggunakan sisi kelemahan manusia dengan menjaga data-data yang bersifat konfidensial.
- Perlu upaya yang keras agar dapat mengubah karakter masyarakat Indonesia agar tidak mudah percaya dan ditakut-takuti oleh orang yang baru dikenal.

5.2. Saran

Berikut ini beberapa saran yang didapat dari penelitian ini :

- Penelitian untuk modus-modus yang paling mutakhir perlu dilakukan untuk melindungi masyarakat dari bentuk kejahatan pencurian identitas.
- Dapat dibuat penelitian lanjutan untuk melihat seberapa besar jumlah perdagangan data oleh pihak ketiga agar dapat dilihat lalu lintas data pribadi seseorang.
- Dapat dilakukan penelitian lebih lanjut tentang cara melengkapi data lewat jejaring sosial.

DAFTAR PUSTAKA

[1] USSAA., "Identity Theft." s.l. : The USAA Educational Foundation, 2005.

[2] Merriam-Webster., identity theft. [Online] 2010. [Dikutip: 23 05 2010.] http://www.merriam-webster.com/dictionary/identity+theft.

[3] Watchtower Bible & Track Society., "Awake." *Someone may Still Your Identity.* March, 2001.

[4] Institute, Insurance Information., Identity Theft. *CONSUMER FRAUD AND IDENTITY THEFT.* [Online] Insurance Information Institute, 2009. [Dikutip: 23 05 2010.] http://www.iii.org/media/facts/statsbyissue/idtheft/.

[5] Papadaki, Maria, Furnell, Steven dan Dodge, Ronald C., *Social Engineering – Exploiting the Weakest Links.* s.l. : European Network and Information Security Agency, 2008.

[6] Granger, Sarah., Social Engineering Fundamentals, Part I: Hacker Tactics. *Symantec.* [Online] 18 12 2001. [Dikutip: 12 05 2010.] http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics.

[7] Rhodes, Colleen., *Safeguarding Against Social Engineering.* East Carolina : s.n., 2006.

[8] AVG Technologies CZ., *Social Engineering:Hacking people,not machines.* s.l. : AVG Technologies CZ, 2009.

[9] Suara Merdeka., "Suara Merdeka." *BI Catat Pemalsuan Kartu Kredit 7.654 Kasus.* [Online] 16 Desember 2009. [Dikutip: 20 05 2010.] http://suaramerdeka.com/v1/index.php/read/news/2009/12/16/42250/BI-Catat-Pemalsuan-Kartu-Kredit-7.654-Kasus.